UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/767,128	01/22/2001	Radia J. Perlman	P4098	2127

45774 7590 05/18/2005

KUDIRKA & JOBSE, LLP
ONE STATE STREET, SUITE 800
BOSTON, MA 02109

EXAMINER
CHEUNG, MARY DA ZHI WANG

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/767,128	PERLMAN, RADIA J.	
	Examiner	Art Unit	
	Mary Cheung	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 February 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) *12-16 and 21-27* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-11,17-20 and 28-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

EA

DETAILED ACTION

Status of the Claims

1. This action is in response to the amendment filed on February 14, 2005. Claims 1-37 are pending. Claims 12-16 and 21-27 are withdrawn. Claims 1-11, 17-20 and 28-37 are examined.

Response to Arguments

2. Applicant's arguments filed February 14, 2005 have been fully considered but they are not persuasive.

Applicant argues that de Silva (U. S. Patent 6,564,320) in view of Hind (U. S. Patent 6,772,331) fails teach at the second node generating a certificate that includes the first identifier that identifies the first node. Examiner respectfully disagrees because de Silva teaches generating a certificate at the second node (column 4 lines 44-58 and column 12 lines 15-19), and Hind teaches generating a certificate at the second node that includes the first identifier (i.e. device identifier) of the first/requesting node (column 9 lines 34-37).

In response to applicant's arguments that de Silva fails to teach time stamp, examiner believes that the time stamp is inherent in de Silva's teaching since de Silva teaches evaluating validity of the digital certificate based on the expiration date.

In response to applicant's arguments that de Silva fails to teach a certificate is untrustworthy based on a comparison of a node identifier in the certificate with the node identifier of an untrustworthy node on a certificate revocation list, this concept is taught

by de Silva as the validity of the currently certificate is determined by making sure the certificate is not revoked (column 4 lines 65-67).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 4-5, 7-9, 11, 17-18, 20, 34 and 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320 in view of Hind et al., U. S. Patent 6,772,331.

As to claim 1, de Silva teaches a method for certificate generation that enables efficient revocation of said certificate, comprising (abstract and column 4 line 65 – column 5 line 10):

At a first node (local server 202 of Figs. 6-8):

- Receiving a request to issue a certificate on behalf of a principal (column 12 lines 3-12 and Figs. 6-8);
- Forwarding said request to a second node, wherein said request includes a first identifier that identifies the first node (column 7 line 40 – column 8 line 18 and column 12 lines 12-15 and Figs. 6-8);

At the second node (central server 104 of Figs. 6-8):

- In response to receipt of the request, generating a certificate (column 4 lines 44-58 and column 12 lines 15-19 and Figs. 6-8).

De Silva does not explicitly teach that the certificate is generated further includes said first identifier. However, this matter is taught by Hind as generating a certificate that includes the identifier of the requesting node (column 7 lines 40-46 and column 9 line 34 – column 10 line 11 and Figs. 1A, 4). It would have been obvious to one of ordinary skill in the art to allow the certificate in de Silva's teachings to include the identifier of the first node because this would allow the system more securely monitoring the generated certificates.

As to claim 4, de Silva teaches authenticating said certificate by said second node (column 4 lines 55-67).

As to claim 5, de Silva teaches authenticating said certificate comprises generating a certificate digitally signed by said second node (column1 lines 48-50 and column 11 lines 34-44).

As to claim 7, de Silva teaches the certificate includes a time stamp that identifies expiration time (column 4 line 65 – column 5 line 10). De Silva does not specifically teach the certificate includes a time stamp that identifies a time associated with the request. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva's certificate to include a time associated with the request because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 8, de Silva teaches authenticating said request by said first node (column 4 lines 41-53).

As to claim 9, de Silva does not explicitly digitally signing said request by said first node. However, de Silva specifically teaches digitally signing the certificate against subsequent tampering (column 1 lines 48-50). It would have been obvious to one of ordinary skill in the art to allow the certificate in de Silva's teachings to be signed by the first node for preventing unauthorized access of the certificate.

As to claim 11, de Silva teaches the certificate includes a time stamp that is associated with expiration time (column 4 line 65 – column 5 line 10). De Silva does not specifically teach the certificate includes a time stamp that is associated with a time and date when said request was received by said second node. It would have been obvious to one of ordinary skill in the art to allow the time stamp in de Silva's certificate to include a time and date associated with said request was received by the second node because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 37, de Silva further teaches revoking untrustworthy certificates (column 1 lines 11-15, 55-58 and column 4 line 65 – column 5 line 10).

Claims 17-18, 20, 34 and 36 are rejected for the similar reasons as claims 1, 4 and 11.

5. Claims 2-3, 6, 10, 19 and 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320 in view of Hind et al., U. S. Patent 6,772,331, and in further view of Vaeth et al., U. S. Patent 6,308,277.

As to claim 2, de Silva modified by Hind teaches said request further includes information related to the principal that requesting a certificate (de Silva: column 12

lines 1-14). De Silva modified by Hind does not specifically state that the information further includes a second identifier that identifies the principal. However, Vaeth teaches this matter (column 4 lines 34-41). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the request information in the teaching of de Silva modified by Hind to include a second identifier that identifies the principal because this would allow the system more securely monitoring transactions among the different terminals for better protecting the secrecy of each transaction.

As to claim 3, the modified method of de Silva and Hind teaches generating a certificate as discussed above. De Silva modified by Hind does not specifically teach said certificate further includes a public key associated with said principal, and said second identifier. However, Vaeth teaches this matter (column 4 lines 34-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow said certificate in the teaching of de Silva modified by Hind further includes a public key associated with said principal, and said second identifier because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 6, de Silva modified by Hind teaches generating a certificate digitally signed by said second node as discussed above. De Silva modified by Hind does not specifically teach generating a certificate digitally signed by said second node using a private key of a public private key pair associated with said second node. However, Vaeth teaches this matter (column 4 lines 34-57). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in the

teaching of de Silva modified by Hind to be signed by using a private key of a public private key pair associated with said second node because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 10, the modified by method of de Silva and Hind teaches the certificate is digitally signed as discussed above. De Silva modified by Hind does not specifically teach the certificate is digitally signed by using a private key of a public/private key pair associated with said first node. However, Vaeth teaches this matter (column 4 lines 34-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in the teaching of de Silva modified by Hind to be signed by using a private key of a public/private key pair associated with said first node because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

Claims 19 and 35 are rejected for the similar reasons as claims 2-3.

6. Claims 28-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over de Silva et al., U. S. Patent 6,564,320 in view of Vaeth et al., U. S. Patent 6,308,277.

As to claim 28, de Silva teaches a computer program product including a computer readable medium, said computer readable medium having a computer program stored thereon for generating a certificate that enables efficient revocation of said certificate, said computer program being executable by a processor and comprising (abstract and column 4 line 65 – column 5 line 10);

a) Program code for receiving a request from a registration authority to issue a certificate behalf of a principal (column 4 lines 34-53 and column 12 lines 6-15 and Figs. 6-8);

b) Program code operative in response to recognition of said request, for generating by a certification authority a certificate authenticated by said certification authority (column 4 lines 44-58 and column 12 lines 14-19 and Figs. 6-8).

De Silva does not explicitly state that said certificate includes at least a principal identifier associated with said principal, a key associated with said principal for use in authenticating messages generated by said principal, and a registration identifier associated with said registration authority. However, Vaeth teaches this matter (column 4 lines 34-61). It would have been obvious to one of ordinary skill in the art at the time the invention was made to allow the certificate in de Silva's teachings to include the identifiers as described hereinabove because this would allow the system more securely monitoring transactions among the different terminals and preventing unauthorized access of the certificate.

As to claim 29, de Silva teaches the program code for generating said certificate is further operative to include within said certificate a time stamp that is associated with expiration time (column 4 line 65 – column 5 line 10). De Silva does not specifically teach the certificate includes a time stamp that is associated with a time of receipt by said certification authority of said request from said registration authority of said request to issue said certificate. It would have been obvious to one of ordinary skill in the art to

allow the time stamp in de Silva's certificate to include a time stamp that is associated with a time of receipt by said certification authority of said request from said registration authority of said request to issue said certificate because this would allow the system more securely tracking each transaction and preventing authentication of the certificate outside the valid time period.

As to claim 32, de Silva teaches the computer program code includes program code for publishing said certificate (column 4 lines 57-58).

As to claim 33, de Silva teaches the program code for publishing said certificate includes program code for forwarding said certificate to a directory server (column 12 lines 14-19).

Claims 30-31 are rejected for the similar reasons as claims 28-29.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Inquire

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mary Cheung whose telephone number is 571-272-6705. The examiner can normally be reached on M-Th (10:00-7:30) Second Friday Off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on 571-272-6712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mary Cheung
Patent Examiner
Art Unit 3621
May 16, 2005

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600